International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC)
ISSN(P): 2250-1568; ISSN(E): 2278-9448
Vol. 4, Issue 1, Feb 2014, 71-78

TRANS STELLAR
• Journal Publications • Research Consultancy

SURVEY OF SECURITY ISSUES IN ROUTING OF MOBILE AD HOC NETWORKS

CHARU WAHI[1] & SANJAY KUMAR SONBHADRA[2]

[1]Birla Institute of Technology, Noida, Uttar Pradesh, India

[2]Shri Shankracharya Institute of Technology & Management, Bhilai, Chhattisgarh, India

ABSTRACT

Mobile ad hoc networks are infrastructure less, pervasive, dynamic, ubiquitous, open and shared medium, distributed environment and no centralized authority. These characteristics make MANET an emerging research area with practical applications. However, unlike wired networks, wireless MANET is vulnerable to security risks due to these unique and fundamental characteristics. Routing plays an important role in the security of the entire network. Early work in the MANET has been primarily focused on developing an efficient routing mechanism, rather than securing such a highly dynamic and resource constrained network. Most of these mechanisms have been developed based on a trusted and cooperative environment. However, the networks are vulnerable in the presence of selfish or malicious nodes to various kinds of attacks. Due to these threats there is a need to develop algorithms and protocols for a secured ad hoc network.

In this article, we highlight the elementary security problem of protecting the network connectivity between mobile nodes in a MANET. We identify the state-of-the-art of security issues related to this problem and discuss the vulnerabilities of ad hoc network. In particular, we emphasize on routing attacks as well as the existing solution schemes.

KEYWORDS: MANET, Vulnerability, Routing, Security, Attacks, Secure Routing

1. INTRODUCTION

A Mobile Ad Hoc Network (MANET) is a group of wireless mobile nodes forming a temporary network without any established infrastructure or centralized authority [1]. Until now, the research focus in MANET has been on developing the routing protocols, improving them for scalability, multi-hop routing and mobility of the ad hoc networks. Though the issues like scalability, mobility, quality of service have their place in wireless network research, the current and future applications of MANET has forced the researcher to look deeply into the security aspects of ad hoc networks [2, 3].

Security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. The security of communication in ad hoc wireless networks is important, especially while deploying MANETs in military applications. The absence of any central coordination mechanism and shared wireless medium makes MANETs more vulnerable to digital/cyber attacks than wired networks [3].

Without proper security, it is possible to gain various advantages by malicious behavior: better service than cooperating nodes, monetary benefits by exploiting incentive measures or trading confidential information; saving power by selfish behavior, preventing someone else from getting proper service, extracting data to get confidential information and so on. [19]

In this article, we study the security issues encountered during routing in MANET. The rest of the article is organized as follows. Section 2 reviews the vulnerabilities of the mobile ad hoc network. In section 3, we talk about different types of attacks on routing. Section 4 surveys the current security solution schemes for MANETs. Section 5 provides

2. VULNERABILITIES OF THE MOBILE AD HOC NETWORKS

Recent surveys on wireless networks indicate that the MANETs are highly vulnerable to security problems than conventional wired and wireless networks [2]. Hence, the existing wired security solutions cannot be used for wireless ad hoc networks. Few researchers have cited few reasons/challenges for the need of new secured routing solutions:-

- **Wireless Medium:** All signals go through bandwidth-constrained wireless links in a MANET, which makes it more prone to physical security threats than fixed networks. Possible link attacks range from passive eavesdropping to active interference.
- **Mobility of Nodes:** Mobile nodes are roaming independently and are able to move in any direction. Therefore, any security solution with a static configuration would not be adequate for the dynamically changing topology.
- **Decentralized Decision Making:** Decentralized decision making in the MANET relies on the cooperative participation of all nodes. The malicious node could simply block or modify the traffic.
- **Limited Energy:** Some or all of the nodes in a MANET may rely on batteries or other exhaustive means for their energy. An attacker could create a new type of DoS (Denial of Service) attack to replay packets to exhaust its energy.
- **Lack of Secure Boundary:** It makes the mobile ad hoc network susceptible to the attacks like network can suffer from weather attacks or link attack that can jeopardize the network.

The features listed above make the mobile ad hoc networks more prone to attacks from the malicious behavior than the traditional wired networks. Therefore, we need to pay more attention to the security issues. Recently several research efforts have been developed to counter against the security attacks.

The ultimate goal of any secured solution is expected to meet the following security requirements:

- **Confidentiality:** Only the authorized receiver/s should be able to access the transmitted data.
- **Integrity:** data Should not be modified during the communication process.
- **Availability:** Network & node services should be available all the time regardless of their state.
- **Authentication:** Participating nodes are legitimate and not impersonators.
- **Non-Repudiation:** Sender of a message shall not be able to later deny sending the message and the recipients shall not be able to deny the receipt after receiving the message [3].

Clearly, security requirements depend very much on the kind of mission for which the mobile ad hoc networks has been deployed [7]. For example, a MANET conceived for military application certainly will have very stringent security requirements as compared to MANET deployed in a conference room or in a lecture hall.

3. ATTACKS ON SECURED ROUTING

The primary objective of an ad-hoc network routing protocol is the correct and efficient route establishment between a pair of nodes so that messages may be delivered reliably and in a timely manner. If routing can be misdirected, the entire network can be compromised. Thus, secured routing plays an important role in the security of the mobile ad-hoc network.

Security always implies the identification of potential attacks, threats and vulnerabilities of a certain system [4]. An attack is an action which aims at compromising the security of the network. There are two major types of attacks in MANET:-

- A **passive attack** does not disrupt the operation of a routing protocol, but only attempts to discover valuable information by listening to routing traffic [4]. They do not influence the functionality of a connection. It's difficult to identify passive attacks because the network operates normally under such attacks.
- An **active attack** is an attempt to improperly modify data, gain authentication or procure authorization by inserting false packets into the data stream or modifying packets transition through the network [4]. They are further classified into internal and external attacks.
- **Internal Attack:** If nodes from within the network are involved, the attacks are referred to as internal attacks.
- **External Attack:** Active attacks when performed from foreign networks are referred to as external attacks.

External attacks in traditional wired networks can be easily prevented and detected by security methods such as firewall. However, because of the dynamic and pervasive nature of an open medium mobile ad hoc network, internal attacks are far more dangerous than the external attacks because the compromised nodes can be the benign user of the network. Some of the active attacks are summarized in Table 1.

Table 1: Active Attacks

Attack	Layer Affected	Description	Proposed Solution
Black-Hole	Network layer	All packets are dropped by sending forged routing packets.	[4], [17]
Wormhole	Network layer	Attacker records packets at one location and replays them at another location.	[15], [8]
Byzantine	Network layer	Nodes are compromised in such a way that the incorrect and malicious behavior cannot be directly detected because of the cooperation among them.	
Resource consumption	Network layer	Consumes the resources of a network	SEAD [9]
Location disclosure	Network layer	Discloses the location of a node	SRP [10]
Flooding		Exhaust network resources to disrupt the routing operation to cause severe degradation in network performance.	[16]
Repudiation	Application layer	Node can deny that it initiated the transaction, which will enable anonymous access ineffective tracking controls.	ARAN [14]
DoS	Multiple layers	Aims to grab the availability of nodes or services of the entire network.	SEAD [9], ARIADNE [11]

4. RELATED WORK

In mobile ad hoc networks, a lot of research has been devoted to routing algorithms. However, in most cases, the nodes are assumed to be cooperative, trustworthy and well-behaved. Initial work on mitigating routing misbehavior in mobile ad hoc networks is proposed in [6]. In this paper, the authors consider the case in which some malicious nodes agree to forward packets but fail to do so. They propose two mechanisms in order to handle this problem: a *watchdog*, in charge of identifying the misbehaving nodes and a *pathrater*, in charge of defining the best route circumventing these nodes. [7]

Hu. et. al. [9] has developed a DSDV based secure routing method called Secure Efficient Distance Vector Routing (SEAD). This method uses efficient one-way hash functions and does not use symmetric cryptographic operations in order to support the nodes of limited CPU processing capability and to guard against Denial-of-Service attacks.

Authors in [10] have proposed the method Secure Routing Protocol (SRP) to handle different forms of attacks, which guarantees correct route discovery, so that fabricated, compromised or replayed route replies are rejected. This method assumes security associations between the end points of a route only, hence bypassing the need to trust intermediary nodes.

The ARIADNE [11] method developed by Hu.et.al. is another important secure on-demand routing protocol. This algorithm prevents attackers from tampering with uncompromised routers consisting of uncompromised nodes. ARIADNE is based on Dynamic Source Routing (DSR) and relies on symmetric cryptography only. It can authenticate messages using one of three ways: shared secrets between each pair of nodes, shared secrets between communicating nodes combined with broadcast authentication or digital signature.

Yi. et.al. [12] propose a new routing technique called Security-Aware Ad Hoc Routing (SAR) that incorporates security attributes as parameters into ad hoc route discovery. This method enables the use of security as a metric to improve the significance of the routes. This approach can be extended to any routing protocol. SAR makes use of trust levels (security attributes assigned to nodes) to make informed, secure routing decisions.

SAODV [13] was introduced to combat the black hole attack. It assumes that each ad hoc node has a signature key pair from a suitable asymmetric cryptosystem. Two mechanisms are used to secure the AODV messages: digital signatures to authenticate the non-mutable fields of the messages, and hash chains to secure the hop count information.

ARAN [14] detects and protects against malicious actions by third parties and peers in an ad hoc environment. It makes use of cryptographic certificates for the purpose of authentication and non-repudiation. It introduces authentication, message integrity and non-repudiation, with the help of cryptographic certificates.

CONFIDANT [18] is a secure on demand routing protocol for making misbehavior nodes unattractive for other nodes to communicate with. It aims at detecting and isolating misbehaving nodes to deny cooperation. CONFIDANT consists of the following components: the monitor, the reputation system and the trust manager.

The table 2 provides the taxonomy developed for identifying the state of research in securing routing in mobile ad hoc networks.

Table 2: Taxonomy of Security Research

Method	Type of Attack	Underlying Protocol	Open Issues
Watchdog/ Pathrater [7]	Routing		Assumes a no priori relationship
SEAD [9]	Authentication, Routing, DoS	DSDV	Packet forwarding
SRP [10]	Authentication, Routing, DoS	Any protocol, but mostly AODV	Unfair utilization of resources
ARIADNE [11]	Authentication, Routing, DoS	DSR	Not optimized
SAR [12]	Authentication, Routing	AODV	Encryption overhead

Table 2: Contd.,

SAODV [13]	Integrity, authentication, non-repudiation	AODV	Fails to detect wormhole attacks
ARAN [14]	Repudiation, Routing	Reactive	Untrusted node, whose certificate is being revoked, may not propagate the revocation message, leading to a partitioned network.
CONFIDANT [18]	Authentication	DSR	Based on global reputation values, which can suffer from inconsistencies in its values or vulnerable to attacks such as advertising false high or low rating about another node
SLSP	Integrity, authentication	OLSR	Gives priority to nodes that have fewer link state updates

5. SUMMARY/CONCLUSIONS

In this survey article, we try to scrutinize the security problems in mobile ad hoc networks. Because of the nature of ad hoc networks such as open and shared wireless medium, mobility of nodes, decentralized decision authority and so on, they are more prone to all kind of security risks. As a result, the security needs in the mobile ad hoc networks are much higher than those in the traditional wired networks.

We briefly introduce the vulnerabilities in the mobile ad hoc networks, most of which are caused by the inherent characteristics of the MANETS. The existence of these vulnerabilities has made it necessary to find some effective security solutions and protect the mobile ad hoc networks from all kinds of security risks. We have pointed out various routing attacks that mainly threaten the connectivity between nodes in a mobile ad hoc network. According to these attack types, we survey several secured routing solutions that can in some way solve the security problems in MANET. This study showed that although many solutions have been proposed, they still are not perfect in terms of tradeoffs between efficiency, scalability, effectiveness, reliability and overall performance of the network.

In mobile ad hoc networks, the most important and constantly needed aspect throughout is the routing service. Therefore it is susceptible to newly emerging attacks anytime. Hence, there is a need to continuously look for new means to defend the routing service against these attacks.

Future research should focus on improving the effectiveness and performance of the security solutions by minimizing the cost to make them suitable for a mobile ad hoc network. In addition, each proposed scheme can counter the effect of a specific attack only and is still vulnerable to other unexpected attacks. Hence, researchers should also explore the possibility of different kinds of attacks and propose a solution to prevent all possible attacks to make a MANET a secure network.

REFERENCES

1. S. Kumar Alampalayam, A. Kumar, S. Srinivasan, "*Mobile Ad Hoc Network Security – a Taxonomy*", 7th IEEE Int'l Conf. on Computer Communications Security, Phoenix Park, South Korea, Feb. 23-25, 2005.

2. L. Zhou, Z. J. Haas, "*Securing Ad Hoc Networks*", IEEE Net., vol. 13, no. 6, 1999.

3. L. Abusalah, A. Khokhar, M. Guizani, "*A Survey of Secure Mobile Ad Hoc Routing Protocols*", IEEE Communiucations Surveys & Tutorials, Vol. 10, No. 4, 2008.

4. H. Deng, W. Li, Dharma P. Agrawal, "*Routing security in Wireless Ad Hoc Networks*", IEEE Communciations Mag., vol. 40, no. 10, Oct. 2002, pp. 70-75.

5. J. Lundberg, "*Routing security in Ad Hoc Networks*", Helsinki University of Technology, http://citeseer.nj.nec.com/400961.html

6. S. Marti et al., "*Mitigating Routing Misbehavior in Mobile Ad Hoc Networks*", 6th Int'l Conf. Mobile Comp. Net., Aug.2000, pp. 255-65.

7. J.-P. Hubaux, L. Buttyan, S. Capkun, "*The Quest for Security in Mobile Ad Hoc Networks*", In Proceedings of the ACM Symposium on Mobile Ad Hoc Networking and Computing (MobiHOC), Long Beach, CA, USA, October 2001, pp. 251-260.

8. Y-C. Hu, A. Perrig and D. Johnson, "*Wormhole attacks in Wireless Networks*", IEEE JSAC, vol. 24, no. 2, Feb. 2006.

9. Y.C. Hu, D.B. Johnson and A. Perrig, *"SEAD: secure efficient distance vector routing for wireless ad hoc networks",* Proceedings of the 4th IEEE Workshop on Mobile Computing Systems & Applications (WMCSA), 2002.

10. P. Papadimitraos and Z.J. Haas, *"Secure routing for mobile ad hoc networks",* SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002.

11. Y.C. Hu, A. Perrig and D.B. Johnson, "*ARIADNE: a secure on-demand routing protocol for ad hoc networks",* MobiCom 2002.

12. S. Yi, P. Naldurg and R. Kravets, *"A Security-aware ad hoc routing protocol for wireless networks",* The 6th world Multi-Conference on Systemic, Cybernetics and Informatics (SCI), 2002.

13. M. Guerrero Zapata, "*Secure Ad-Hoc On-Demand Distance Vector Routing*", Mobile Computing and Comm. Review, vol.6, no. 3.

14. B. Dahill et. al., "*ARAN: A Secure Routing protocol for Ad Hoc Networks*", UMASS Tech. Report, 2002, pp. 2-32.

15. Y.Hu, A. Perrig, D.B. Johnson, "*Packet Leashes: A defense against Wormhole Attacks in Wireless Ad Hoc Networks*", Proc. IEEE INFOCOM 2003, vol. 3, Apr. 2003, pp. – 1976-86.

16. P.Yi et al., "*A new routing attack in Mobile Ad Hoc Networks*", Int'l, J. Info. Tech., vol.11, no.2, 2005.

17. S. Kurosawa et al., "*Detecting Blackhole Attack on AODV-Based Mobile Ad Hoc Networks by Dynamic Learning Method*", Proc. Int'l. J. Network Sec., 2006.

18. S. Buchegger and J.L. Boudec, "*Performance Analysis of the CONFIDANT Protocol Cooperation of Nodes Fairness In Dynamic Ad-Hoc Networks"*, Proc. IEEE/ACM Symp. Mobile Ad Hoc Networking and Computing (MobiHOC), 2002.

19. S. Buchegger and J.L. Boudec, "*Nodes bearing grudges: towards routing security, fairness and robustness in mobile ad hoc networks"*, Proc. 10th Euromicro Workshop, 2002.